PNNL-32928

PISCES 4th Annual Academic Workshop

April 22, 2022

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy under
Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <https://www.ntis.gov/about>
Online ordering: http://www.ntis.gov

PNNL-32928

PISCES 4th Annual Academic Workshop

April 22, 2022

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Acronyms and Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
CWU	Central Washington University
DHS	Department of Homeland Security
EWU	Eastern Washington University
IDS	Intrusion Detection System
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
PISCES	Public Infrastructure Security Cyber Education System
PNNL	Pacific Northwest National Laboratory
SIEM	Security Incident and Event Management
SOC	Security Operations Center
WWU	Western Washington University

Contents

1.0 Overview

On April 22, 2022, the 4th Annual Public Infrastructure Security Cyber Education System (PISCES) Academic Workshop convened program participants in a virtual forum to discuss program operations.

The workshop aimed to sustain momentum toward providing critical cybersecurity analysis to public sector organizations in developing a high-quality cybersecurity workforce. Workshop participants reviewed the current PISCES effort and opportunities for improvement, including:

- Enhancing, standardizing, and sharing curriculum.
- Conducting outreach to engage new partner universities and communities.
- Improving sustainability within the program model.

The event featured both broad discussions and breakout sessions designed for new and experienced users. Discussion topics included an overview of the current effort and a demonstration of the PISCES system, reports from participating schools, student feedback, and a review of the PISCES curriculum, research initiatives, Community Liaison role, and club.

About PISCES

PISCES provides a data-sharing network to small communities in need of critical cybersecurity analysis. Students at qualified educational institutions studying cybersecurity analyze this data to provide live insights to communities about their network security.

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the Pacific Northwest National Laboratory (PNNL) provide support in pursuit of PISCES' three principal objectives:

- Provide cybersecurity monitoring and analysis services for underserved public sector organizations.
- Develop a reliable pipeline of high-quality entry-level cyber professionals ready for the workforce.
- Conduct research projects to improve event detection and incident management.

This report summarizes the workshop discussions organized by presentation, including question and answer sessions. Video segments from the workshop are available on the PISCES website at https://pisces-intl.org.

2.0 Welcome and Introductions | Erik Fretheim, Western Washington University

Erik Fretheim, Western Washington University (WWU), delivered welcome remarks, emphasizing the vital role PISCES has in building next-generation analysts to protect the nation's cybersecurity. Even the best preventive controls will fail, which is why analysts are needed to watch events, to observe and catch the threat surge in real time. While technology may automate some aspects of the job, cyber analyst is reportedly the 10th growing job in the nation[1]. To succeed in the role, analysts need hands-on training with real-world data—and that is where PISCES fills a crucial capability gap. By partnering with colleges and universities, PISCES is providing operational experience to developing analysts while providing critical services to small municipalities that could otherwise not afford it. Fretheim also shared that PISCES continues to expand to new states and the process for doing so. Ideally, PISCES leaders connect with the state government, establish a connection with universities and local governments, and operations begin with a goal to transition maintenance costs to the state—this is the foundation of PISCES's sustainability model.

Fretheim closed by introduced partnering organizations participating in the workshop, including CISA, CI Security, PISCES-Intl., and PNNL and university partners Central Washington University (CWU), Eastern

[1] https://www.bls.gov/ooh/fastest-growing.htm

Washington University (EWU), Western Washington University (WWU), Metropolitan State University of Denver (MSU), University of Kentucky (UKY), Spokane Community College (SCC) and many others.

Following Fretheim's introduction, PISCES co-founder Mike Hamilton shared the 10-year history of PISCES, from the early days of the Public Regional Information Security Event Management System[1] to the current model with five academic partners and 11 jurisdictions. The project was created to perform monitoring for local governments, which typically lack sufficient infrastructure monitoring. PISCES creators recognized the need for monitoring at the local level and the opportunity to involve students at WWU and the University of Washington. Hamilton cited the many contributors who aided the effort over the years, including the City of Seattle, DHS Science and Technology Directorate, Washington State Office of the Chief Information Officer, and PNNL.

2.1 Opening Remarks | Toni Benson, Cybersecurity and Infrastructure Security Agency

Toni Benson, CISA Cyber Defense Education and Training, shared the CISA goal to reduce national risk is challenged in part by the long-standing cyber workforce shortage and gap. She noted recent issues in ransomware and other national-level incidents demonstrate the need for trained individuals who can fill in the gaps and shore up the nation. Unfortunately, recent graduates typically lacked the technical experience or hands-on keyboard work required of analyst's roles. PISCES is one tool helping give students that necessary experience. "We see the shortage of qualified cyber professionals as a national security issue. [Through PISCES] We're giving them real-life experience. It's an opportunity for students to get the experience at the outset and have the expectation to see things on the network and know how to respond," said Benson.

2.2 Keynote Address | Greg Bianchi, Microsoft Philanthropies

Keynote speaker Greg Bianchi, Microsoft Philanthropies, shared what excites him about PISCES: The program provides students actual workplace experience with real data in real time. Given the national focus on digital inclusion to upskill and help graduating students succeed in the digital economy, given students the skills they need takes a different level of cyber education and Microsoft looks to build on its education partnership by adding PISCES to the mix. Bianchi underscored the critical skill gap in protecting public and private infrastructure and shared, "We are focused on bench building to do more and do it faster, and we are grateful for PISCES and the role they're playing to address the gap." Citing the nation's 500,000 open cybersecurity jobs, Bianchi shared Microsoft has committed to skill 250,000 people in cybersecurity by 2025.[2] Part of that effort includes offering free curriculum and certification, training for community colleges, and scholarships and supplemental resources. During discussions, participants concurred that an analyst certificate, particularly one that documents and makes easily identifiable that students have operational experience, will be of great value in students' post-PISCES employment pursuits.

3.0 PISCES Highlights | Mike Hamilton, CI Security

Hamilton briefly discussed the evolution and importance of PISCES to protecting local government infrastructure. The critical systems—water, traffic, communications, elections—are all held up by information technology and prevention measures will eventually fail.

To better understand the program's operations and ultimately its success, Hamilton gave an overview of the mathematics of risk in the context of PISCES. Essentially, risk is the product of likelihood and impact, and it

[1] https://ocio.wa.gov/news/prisem

[2] https://aka.ms/cyberskills

can be lowered or the likelihood that a threat will occur can be reduced with preventive control (firewalls, filtering, user training, managing vulnerabilities, etc.). When that happens, the equation switches to impact. The solution to reduce impact is to see what is happening on the network and address it immediately. Unfortunately, detection and response is a significant gap. This is where intrusion detection systems (IDSs) and PISCES play an important role. Hamilton gave an overview of how an IDS works in general and with PISCES. PISCES configures, ships, and puts a collector or network tap on the community partner network. The network tap is the telemetry point for everything that moves from internal network to the internet. In addition to IDS alerts, PISCES pulls packet headers off the packets. Netflow and IDS alerts are shipped to Poulsbo Cyber Range for review with critical insight analytics engines. Hamilton emphasized throughout this process, no one sees actual content, only metadata. Metadata allows students to search around an event.

On that note, Hamilton shared several highlights from the program's recent operations. In March 2022, PISCES ingested in excess of 300Tb from 10 community partner organizations. Nearly 152 million IDS alerts, 162 student tickets were generated from that traffic, a PISCES Senior Analyst provided oversight to the tickets, and 12 events were reported to the community partners for resolution. He also shared examples of specific events reported and accomplishments from the past year.

Hamilton also shared that the program launched a new monthly report to update stakeholders on program operations and anonymized findings. The reports include:

- Narrative description
- Volume of traffic ingested
- Raw number of alerts
- Tickets/investigations by student analysts
- Specific events report to customers
- Additional bulletins or vulnerability alerts

Hamilton also highlighted the STIX/TAXII Automated Threat Signatures capability. The structured threat information exchange allows for exchange of source and destination addresses, ports, bytes moved, protocol moved, time of occurrence, malware identified, etc. The information is fed to the server and shared to connected servers, automating information sharing across a wide geography. Looking forward, this will create efficiency to aid construction of a detection signature.

4.0 Breakout Discussions

The event featured a series of breakout sessions designed for new and experienced PISCES participants. Students, professors, community representatives, and many others discussed key topics such as the future of PISCES, the progress of the curriculum, and the continued development of the program.

4.1 What is PISCES?

PISCES provides qualified students with curricula and supervised experiences to act as entry-level cyber analysts. Students analyze streaming data for small communities or municipalities who may otherwise not be able to obtain cybersecurity to the extent needed. Through PISCES, a reliable high-quality pipeline is being developed to address the shortage of cyber professionals ready for the workforce. At the request of DHS CISA, PNNL and PISCES developed an operational capability that will:

- Develop college-level curricula using "live" streaming data to train and educate students as cyber analysts while providing cyber analysis for small and rural communities

- Provide the data-sharing agreements and infrastructure to provide streaming data to participating colleges
- Develop, test, and implement the business model or models that will provide financial sustainability for the enterprise
- Develop the roadmap to transition the operational capability from regional deployment to national deployment

PISCES then worked with WWU to develop and teach appropriate curricula, developed a data exchange network allowing net flow to be streamed from small communities that cannot afford to pay for cyber analysis, and built out the infrastructure to stream data to qualified educational institutions.

4.2 Curriculum Overview

Michael Tsikerdekis, WWU, provided an overview of PISCES visualizations and dashboards, what they do, and what is still needed. He cited a need for improved visualizations guidance, security incident and event management (SIEM), and reporting.

Dashboards

While all PISCES schools make visualizations and dashboards to represent their findings and operations, Tsikerdekis noted some dashboards are not as insightful or useful as others. Unfortunately, employers increasingly desire that students can demonstrate productive dashboard and visualization skills or experience. Thus, the discussion focused on suggestions for measurable improvements.

Participants shared they suggestion students build dashboards too look at the important data they want to observe. It was suggested that PISCES could bring in industry professionals to discuss dashboards with PISCES partners.

Security Incident and Event Management

Tsikerdekis shared that industry is using SIEM software (some automated, some manual). Kibana supports this but PISCES does not have it enabled. Given PISCES students are starting from the ground level, Tsikerdekis posed the question if there is curriculum capacity for analysts to learn this feature.

Alan Carter noted his university is planning a second class and would be interested in including SIEM. His students start with the CISCO cyberops analyst course and look at traffic in it. Cyberops goes through 'security onion,' dashboards, and Kibana. Carter noted he is CISCO trainer and has relationship with local area representative who can help as school become a CISCO school. Cost is minimal. Interested partners can contact Carter for additional information.

5.0 Security Operations Center Course | Deborah Wells, Central Washington University

Deborah Wells, CWU, provided an overview of the SOC course. Currently in operation at CWU, the course essentially provides a follow-on to the PISCES curriculum, where students gain an understanding of how a SOC or virtual SOC [VSOC] operates. The course shares the fundamentals of SOC operations, including an introduction to the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) framework.

- Explain SOC operations and capabilities, including virtualization

- Integrate teamwork into a SOC
- Better understand networking and how it ties into defense-in-depth strategy
- Analyze traffic, understand what is happening, and provide a path forward for better security optimization
- Assessing metrics produced from SOC/VSOC and provide critical assessments
- Perform threat hunting using manual or machine-assisted techniques
- Prepare/construct incident response plan/checklist and understand SIEM
- Determine plausible network defense strategy for city/municipality
- Align SOC methods to NIST/NICE Framework

The course can be designed to be taught prior to the PISCES project and all it entails, or it could be taught after PISCES. It would be appropriate for a 300-400 level course, or it can be modified for a graduate-level course by adding more research and analytical assignments. The learning modules are outlined in Table 1.

Table 1. SOC Course Learning Modules

Module	*Topic*
Module 1	Introduction to SOC and virtualization
Module 2	NIST/NICE framework
Module 3	Team building and a SOC
Module 4	Security tools, security environment, vulnerability scans
Module 5	Single pane of glass – Security information and event management, Managed detection and response, and Managed Security Service Providers
Module 6	Introduction (or continuation) of PISCES
Module 7	Log analysis in depth
Module 8	Incident response, playbooks
Module 9	Threat intel, threat hunting, forensics
Module 10	Advanced monitoring PISCES, automation, artificial intelligence, APIs
Module 11	Purple Team, Red Team, Blue Team
Module 12	Putting it all together, jobs in a SOC, managing a SOC
Final Assessment	Virtual SOC

During discussion, Hamilton noted that it would be great if there were sufficient universities teaching SOC after PISCES analyst course that students could collaborate—which is something they have oft cited as beneficial. Colorado participants also suggested exploring the Clark database to distribute the PISCES curriculum. They are currently using the cybersecurity diversity education curriculum and interacting with the Clark database.

Wells concluded the session sharing that the course curriculum is available for use. Materials include a draft syllabus, assessment and quizzes, rubric, videos, 12 modules, and a final assessment. Wells noted she anticipates having the course curriculum finalized and available for use in June 2022. Academic partners interested in teaching the course can contact PISCES for more information.

6.0 Community Liaison Observations | Mike Hamilton, CI Security

Hamilton provided an overview of the Community Liaison role, a paid position that is crucial to working with communities. The Community Liaison is the person who communicates with community partners.

At present, the expectations of the role include:

- At least one Community Liaison for every regional deployment
- Managing no more than five universities
- Acts, in part, as a teaching assistant
- Compensates for student outages
- Knowledge of networking and stack operations

The responsibilities of the role include:

- Review student tickets
- Provide feedback to students
- Validate findings
- Make customer contact
- Follow up
- Conduct independent investigations

Hamilton shared common issues the Community Liaison observes with customers, such as incomplete information, and student tickets, such as mis-labeling or mis-escalating. Fortunately, he noted the wide variability in student tickets notably improves as the semester or quarter progresses and the Fusion Center continues to provide useful threat information (i.e., indicator lists) for use by students. Participants concluded the session with a discussion of the potential for defining new community metrics to help measure PISCES's success, such an activity metric that would translate the general amount of tickets to be expected for a network for a particular size.

7.0 Success Stories | Steve Stein, PISCES-Intl.

Steve Stein, PISCES-Intl., shared recent success stories from PISCES' expansion to two new states: Colorado and Kentucky. Together, these partnerships represent a positive expansion leveraging lessons learned from previous expansions.

For Colorado, PISCES connected with the Colorado National Cyber Center (also a non-profit organization). PISCES and the center connected to state government and, with the help of CISA and PNNL, secured federal funding for a partnership. Ongoing funding will require a commitment from the state to provide long-term sustainability funding. Together, PISCES conducted a webinar with academics in Colorado and potential data-sharing partners. This proved to be an efficient way to disseminate the PISCES opportunities. At present, the lead academic partner is Metropolitan State University in Denver, which has 15 students participating, and Pueblo Community College is also participating. Metropolitan State University has physically built a SOC with support from a private commercial partner, where students have the opportunity for paid internships in the SOC.

In Kentucky, PISCES immediately connect with state leadership to commit to out-year funding to sustain PISCES longer term. University of Kentucky is the lead academic institution with several others interested. To date, Kentucky has held two webinars to engage others in the state and will begin implementing the curriculum in Fall 2022.

8.0 Student Feedback

Recent PISCES students from CWU and WWU shared their experiences in the program and provided recommendations for improvements. Collectively, students indicated that a refresher course on cyber basics would be beneficial as the timing of the course may be very distant from their introductory coursework. Suggested content could include networking (ports, protocols, etc.) and knowledge of what IDS signatures are, how to write them, what they do, etc. This might also enable more competent students analysts from the outset. Additionally, a student currently pursuing SOC jobs noted that SOC analysts jobs typically require 3-5 years of experience. He suggested that perhaps if the skills and unique nature of the program were better communicated to industry, employers may be more interested in hiring PISCES students.

When asked if they felt like they made a difference to their municipality, students indicated they felt like they were contributing to the bigger cybersecurity mission of their community. While many findings may be false positives, they noted it was beneficial to participate. For example, having tickets reported to the city, they made a valuable contribution. They noted it would be more impactful if they could see, to an extent feasible, what happens after they escalate a ticket.

Regarding communication with other colleges and universities, students cited a few examples of collaborating with others to understand what other were seeing in their jurisdictions. It was suggested that perhaps assigning students across jurisdictions or universities could foster greater collaboration. Cross-university collaboration could also help build both PISCES's and the students' network. Wells noted that in her course she requires teaming and collaboration, as it is a common part of the job and looking at other tickets exposes students to how others operate.

Lastly, students collectively concurred that they looked at or reverse engineering other students' materials to inform their own learning and future operations. Using historical tickets was also cited as very beneficial. Knowing who you are working with can also help build your network.

9.0 PISCES Club | Eric Fretheim, Western Washington University

Fretheim gave an overview of the PISCES club concept, established to sustain student participation beyond the PISCES course while also sustaining PISCES knowledge and monitoring across academic breaks. To participate, students must have completed a PISCES course, be enrolled in college/university, and have permission from an instructor (to be renewed each academic term). Club members are expected to monitor and update the Club Wiki, monitor networks and work with tickets, maintain operational security, and mentor other students when possible. Instructors are expected to validate students (confirm students meet club requirements), address performance issues with students as necessary, and maintain non-disclosure agreements.

Fretheim emphasized the PISCES club was launched out of a desire by students to continue with analysis after the course concludes. Fretheim shared how in addition to maintaining student interest, the club provides coverage during academic breaks and mentorship to new students. The club was initially open to students who completed the course while still enrolled in their university. The goal is to create a state-wide club with a coordinator to take the burden off the universities. Initial steps have entailed selecting students to continue in the system, establishing a Slack channel for communication, and maintaining informal management by instructors. Some schools have also used the club as an internship opportunity. The next priority is to secure resources to serve as the club coordinator.

10.0 PISCES Research | Brennan Vanden Bos, Western Washington University

Brennan Vanden Bos, WWU, shared his recent research into what factors affect ticket resolution time and how students interact with each other. Generally, Vanden Bos's research indicated time to resolution has decreased over time, groups of tickets are being marked resolved at the same time, and the average time active is just over 30 days. Additionally, he explored unique users versus time to resolution and found the more unique users, the longer time active and researched social network analysis and interactions. Looking ahead, he plans to conduct more investigation into why more unique users on a ticket correlates with increased time to resolution and characteristics of non-instructor users with high betweenness-centrality.

Tsikerdekis highlighted the opportunity for additional PISCES graduate research. Universities participating in PISCES have the data and opportunity. Further, opportunities are increasing to connect academia and business. On this note, Tsikerdekis posed the question of how more may be done with the PISCES data, if approved? Hamilton noted a research component is noted in the PISCES service agreement. Furthermore, PNNL has a suite of tools that may be applicable to put higher-quality information in front of analysts—it was proposed that PISCES partners should participate in a technology briefing with the laboratory.

11.0 Wrap-Up / Q&A

Key points of the wrap-up discussion addressed:

- The potential to look at data from small jurisdictions to provide a set of statements or case studies that exemplify why it is important to monitor and protect our communities.
- The potential for ingesting full header email data to be able to do more, such as address forged email, injected threat email, etc.
- Compile data incoming from other countries, demonstrating how Washington State jurisdictions are impacted from illicit overseas attackers.

12.0 Conclusion and Next Steps

Key takeaways and next steps garnered from the day's discussion included:

- Defining a path forward for PISCES or analyst certification opportunities
- Exploring tools like the Clark databases to share the PISCES curriculum
- Hosting a technology briefing or open house to share PNNL technologies and opportunities with program participants.

Looking forward, the PISCES teams will explore these ideas further and incorporate participants' feedback into their curriculum, partnering model, and operations. Key tasks to

Appendix A – Agenda

Time	Topic	Presenter
9:00 a.m. – 9:20 a.m.	Welcome and Introductions	Erik Fretheim Mike Hamilton
9:20 a.m. – 9:25 a.m.	Opening Remarks from CISA	Toni Benson
9:25 a.m. – 9:45 a.m.	Keynote Address	Greg Bianchi
9:45 a.m. – 10:15 a.m.	PISCES Highlights • Positive statistics • Positive municipality outcomes	Mike Hamilton
Break		

Track 1			Track 2		
Time	**Topic**	**Presenter**	**Time**	**Topic**	**Presenter**
10:30 a.m. – 10:45 a.m.	What is PISCES?	Erik Fretheim	10:30 a.m. – 11:00 a.m.	Update on Dashboards and Visualizations	Michael Tsikerdekis
10:45 a.m. – 11:30 a.m.	Curriculum Overview/How it works	Erik Fretheim	11:00 a.m. – 11:30 a.m.	Curriculum Update and Feedback	Michael Tsikerdekis
Break					

Time	Topic	Presenter
12:30 p.m. – 1:00 p.m.	SOC Course	Deborah Wells
1:00 p.m. – 1:15 p.m.	Community Liaison • Items of interest ▪ Role evolution	Mike Hamilton
1:15 p.m. – 1:30 p.m.	Highlight: CO and KY success stories	Steve Stein
1:30 p.m. – 2:00 p.m.	Student Feedback	Students from ▪ Central Washington o Neal Burfitt o Drew Neuser ▪ Eastern Washington ▪ Western Washington o Lyndsey Pettit o Jared Larson o Brennan Vanden Bos
2:00 p.m. – 2:10 p.m.	PISCES Club	Erik Fretheim
2:10 p.m. – 2:40 p.m.	PISCES Research Discussion • Michael's ticket project – 10 mins. • Addy Moran – 10 Mins. • Brainstorm new ideas	Michael Tsikerdekis Brennan Vanden Bos

2:40 p.m. – 2:55 p.m.	Round Robin / General Q&A	Erik Fretheim
2:55 p.m. – 3:00 p.m.	Closing Remarks & Adjourn	Erik Fretheim Mike Hamilton

Appendix B – Participants

- Toni Benson, Cyber and Infrastructure Security Agency
- Greg Bianchi, Microsoft Philanthropies
- Erik Fretheim, Western Washington University
- Mike Hamilton, CI Security
- Steve Stein, PISCES-Intl.
- Michael Tsikerdekis, Western Washington University
- Deborah Wells, Central Washington University
- Jessica Gray, Pacific Northwest National Laboratory
- Christian Perry, Pacific Northwest National Laboratory
- Amariah Jackson, Pacific Northwest National Laboratory
- Sam Ortega, Pacific Northwest National Laboratory
- Maren Disney, Pacific Northwest National Laboratory
- Brennan Vanden Bos, Western Washington Laboratory
- Neal Burfitt, Central Washington University
- Drew Neuser, Central Washington University
- Lyndsey Pettit, Western Washington University
- Jared Larson, Western Washington University

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov